2012

National Security in the Information Age

Rosa Brooks

Georgetown University Law Center, rosa.brooks@law.georgetown.edu

Georgetown Public Law and Legal Theory Research Paper No. 13-044

Rosa Ehrenreich Brooks, National Security in the Information Age, in ECONOMICS AND SECURITY: CHALLENGES AND OPPORTUNITIES IN A RESOURCES CONSTRAINED WORLD (Newport, R.I.: Naval War College forthcoming)

Rosa Brooks

National Security in the Information Age

Ruger Workshop

Naval War College

3 November 2011

"Talk is cheap." We've all heard that, and perhaps it helps explain the recent surge of interest in strategic communication (SC) and information operations (IO). With the global economy in crisis and the US defense budget on the chopping block, it's tempting to look to strategic communication (SC) as a low-cost way to help advance US national security interests. Communication certainly *sounds* like something inexpensive—at least relative to major weapons systems and spiraling health care costs.

But effective strategic communication is more than just talk. (And to the extent that it *is* "just talk," it's definitely cheap—and you get what you pay for, but not in a good way). Getting SC and IO "right" isn't easy, and will require significant new investments (not on the order of the Joint Strike Fighter, perhaps, but still significant). And even then, strategic communication and information operations offer no panacea.

Let me start by contextualizing the environment in which discussions of strategic communication and information operations now occur. Nick Burns has already outlined the increasingly complex security environment in which we now operate. In the world we live in, we're seeing the impact of rapid but uneven globalization, rapid and unpredictable technological development (including the development of WMD technologies); increased interconnectedness and interdependence between states; the erosion of traditional boundaries between foreign and domestic, civilian and combatant, state and non-state actors, and war and peace. We're seeing the increasing prevalence of hybrid and asymmetrical forms of warfare, and more and more threats emanating from failed states or ungoverned spaces, as well as from state actors. In general, we see non-state actors (good and bad) playing a greater role, and we must increasingly reckon with the rise of globally diffuse terrorist networks and other transnational threats. Throw in tensions in the global commons, climate change, demographic trends (such as youth bulges and aging societies) and, of course, the global economic downturn and increasing resource scarcity. The bottom line: our world is growing ever more complex and unpredictable.

The information environment has been changing right along with the broader security environment. Today, the information environment connects almost everyone, almost everywhere, almost instantaneously. The media environment has become global, and there's no longer such thing as "the news cycle" – everything is 24/7. Barriers between US and global publics have virtual disappeared: Everything and anything can "go viral" instantly, and it's no longer possible to say one thing to a US audience and another thing to a foreign audience and assume no one will ever set the statements side by side. The Pakistani military has a very clear idea of what the Secretary of Defense tells Congress about Pakistan, for instance — and Congress has an equally clear idea of how Pakistani leaders talk about the United States to their domestic constituencies.

Technological changes and lower costs have also democratized the media and information environment: internet and cell phone access is increasingly ubiquitous, and individuals and organizations are ever-more reliant on electronic communication. Today, news, commentary, and video can be produced and accessed equally by first world media producers, Washington decision-makers, Iowa housewives, Afghan shepherds, Chinese university students, Colombian insurgents, and Al Qaeda members.

As with the security environment more broadly, the rapidly changing information environment creates both new challenges and new opportunities for the US government. I should emphasize that this is true across the executive branch. All USG agencies, from Defense to State to Treasury and beyond, are struggling to adapt anachronistic programs and policies.

Obviously the Defense Department's core objective remains unchanged. DoD's constitutional and statutory mission is to defend the nation -- to prevent, prepare for, and prevail in conflicts. This means, among other things, that DoD needs to be able to operate effectively in the rapidly changing information environment. More concretely, DoD needs to be able to act in the information environment to engage, inform, persuade, and influence a wide range of audiences and stakeholders.

DoD needs to engage and inform allied and friendly audiences about national and military objectives: about who we are, what we're doing, and why it matters. DoD also needs to be able to engage, inform, persuade and influence neutral audiences: ideally, we want to persuade neutral audiences to become allies, but at a minimum, we want to dissuade them from aiding or joining our adversaries. And finally, DoD needs to influence our adversaries: we want to discourage, demoralize, confuse and deceive our adversaries at every level, and we want to corrupt, disrupt or usurp our adversaries' ability to communicate and make decisions that will hurt us. A corollary to that is that we need to protect our own communications, information systems and decision-making from adversary attempts to influence, corrupt, disrupt or usurp them via manipulation of the information environment.

In many ways, there's nothing new here. Nations and militaries have always sought to operate in the information environment, from the time humans communicated using smoke signals to the World War Two era of cryptography and psychological warfare. Allied efforts to mislead Germany about the timing and location of the invasion of Normandy remain a classic example of a successful military deception campaign, and Allied pamphlet drops to German troops remain a classic example of PSYOP. What's changed isn't the *necessity* of operating in the information environment—what's changed is the means through which that can be done.

Today, the Defense Department has many activities and programs designed to achieve effects in the information environment:

- Military exercises with partners send messages about U.S. readiness and commitments
- Electronic warfare platforms jam adversary radar to disguise the intent of friendly aircraft and confuse adversary decision-makers
- The use of female screeners on raids in Afghanistan is intended to communicate U.S. respect for local cultural norms
- Posters and billboards in Iraq help civilians identify and report possible IEDs
- Speeches by DoD senior leaders communicate national and DoD objectives to a domestic and foreign audiences

- Computer network operations disrupt adversary websites and email communications
- DoD-sponsored websites seek to provide a truthful, alternative news and information source as a counter-weight to extremist information sources, and viewer comments and usage statistics provide us with situational awareness
- Media training for community leaders in Afghanistan enables them to be more effective advocates of USG-supported goals
- Building and securing cell phone towers in Kandahar reduces Taliban ability to prevent the population from communicating with outsiders.

Note how varied and diverse those examples are. Defense efforts to operate in the information environment are often divided into two categories: the cognitive and the technical, although it's a somewhat artificial distinction. But computer network operations and electronic warfare are primarily technical in nature (though they are intended, secondarily, to achieve cognitive effects), while speeches and billboards are primarily cognitive in nature: their main goal is to change an audience's thinking (and, ultimately, behavior) through facts and arguments.

In the remainder of these remarks, I'm going to focus primarily on the cognitive aspects of SC and IO; the technical aspects—particularly cyber—present somewhat different issues, and it's beyond the scope of these short remarks to address those issues. Suffice it to say that DoD has many tools for operating in the information environment. We use different labels for those tools at different times: sometimes we talk about SC or IO, sometimes about Public Affairs, sometimes about PYSOP or Military Information Support Operations. I don't want to get into the semantic issues here—that's a rabbit hole down which many fine people have disappeared forever. I'll be speaking generally about SC, which can overlap on an operational level with IO. What I do want to do is highlight some key insights about strategic communication, insights we need to keep in mind if we're tempted to see SC as a cheap and easy way to further our security interests in an age of resource constraints. Then I want to highlight a few areas in which we need to invest additional resources, if we want SC to be effective.

Eight Key Insights:

Before getting to investment areas, let me offer eight insights about effective strategic communication.

1. **E*verything* communicates *something*.** When people hear the term "strategic communication," the word "communication" often makes them think of "communications," which in turn makes them think of press releases, talking points, and other kinds of "messaging." These can be a vital part of strategic communication, but words aren't the only way we communicate. Far from it. Everything we do and say produces effects in the information environment, and much of the time, actions speak louder than words. Kinetic strikes, force posture, humanitarian aid – all these send "messages," though we sometimes forget this.

2. **The message each audience receives is not always the message we intended to send.** People filter new information through their pre-existing beliefs. Obviously, we can't control how people hear and interpret our messages—but what we can do, and must do, is *plan* our information programs and other activities to maximize the likelihood that they will produce the information effects we want… and minimize or mitigate unintended effects. Doing this requires constant efforts to understand the information environment – both its technical

dimensions (What technologies do people and organizations of interest rely on? How do they work? What are their quirks and vulnerabilities?) and its cognitive dimensions (people's perceptions, beliefs and their impact on decisions and behavior; the social networks through which communications flow). It also requires constant efforts to coordinate, de-conflict, synchronize & integrate our actions and words (to avoid send mixed messages or committing "message fratricide.") Good strategic communication is "receiver-centric," not 'sender-centric."

3. **Actions speak louder than words.** When our actions seem at odds with our words, we get problems. (When we say, "The US does not torture," for instance, but Abu Ghraib photos tell a different story). Some call this the "say/do gap," and it's nearly always fatal to efforts to get our message across. Effective strategic communication doesn't require us to convince the rest of the world to like us—but it does require that others perceive the United States government as credible. When big say/do gaps exist, we lose all credibility.

4. You can't have strategic communication if you don't have a strategy. SC isn't magic pixie dust. You can't sprinkle it on a problem to make it go away. If the true problem is that we don't have a clear idea of what we're doing and why (why we're intervening in Libya; how we see China; whether we want to contain or challenge Iran, etc.), no amount of "strategic communication" will get Congress, the American public, allies or our potential adversaries off our backs. Strategic communication, by definition, has to be integrated into a broader strategy. If it's not, it's just "messaging," and will probably not accomplish much. (It can even hurt, when a say/do gap is created). To put it differently: you can put lipstick on a pig, but it's still going to look like a pig.

5. We're not in a war of ideas. The "war of ideas" metaphor is one that should be tossed into history's dustbin. Not only does it presuppose conflict where there may not be any, it dangrously misunderstands and oversimplifies the relationship between ideas, attitudes and behavior.

At the end of the day, we care about strategic communication not because we care about the internal mental state of of audiences and stakeholders—we care about strategic communication because we want audiences and stakeholders to *behave* in certain ways and refrain from behaving in other ways. We want others to help us, or, at a minimum, to refrain from helping our adversaries. We want adversaries to stop trying to damage our interests. But we don't always understand the role that information or "ideas" plays in motivating behavior.

It's rarely simply: reading a book, hearing a sermon, or watching a video is unlikely to turn an ordinary young man into a committed terrorist, for instance, unless quite a few other factors are pushing him in the same direction. People and ideas don't exist in a vacuum: people are part of families, tribes, nations, religions, ethnic groups, social networks, and professions – and they are products of their educational systems, their economic systems, their cultures, and their histories. The literature on radicalization suggests that some complex interaction of all these factors is what leads to violent behavior in some individuals. "Ideas" and emerging ideologies aren't irrelevant, but neither are they necessarily central to what makes a particular individual join Al Qaeda or fight with the Taliban. To paraphrase the National Rifle Association: ideas don't kill people, people kill people. The "war of ideas" metaphor leads us to focus on developing "counter-narratives," often to the exclusion of the many other factors that probably have far more impact on behavior.

6. We need to become more culturally, historically and linguistically sophisticated. Whether we want to construct counter-narratives or understand the many other factors that influence audience and stakeholder attitudes and behavior, we need to ge better at understanding other cultures. The late Richard Holbrooke famously complained that the US—the quintessential communications society-- was being out-communicated by a guy in a cave. As I've just said, though, being good at selling soda, making movies people like to watch or winning elections doesn't necessarily translate into being good at changing the complex, bundled attitudes and behaviors of millions of people in foreign countries. What's more, Osama bin Ladin started out with the home court advantage: and to state the obvious, it's much easier to change the minds and behaviors of people you understand.

They say all politics is local: perhaps all strategic communication is fundamentally local, too. To sell a consumer product—or al Qaeda, for that matter— it sure helps to know the human terrain, as the military puts it. It helps to know the local language, the history, the narratives that resonate in people's minds, the day to day pressures, the long-nurtured grievances, the cherished hopes. If you don't know these things, you make mistakes. You sound klutzy, overbearing, tone-deaf, or simply ridiculous.

7. This is a long game, and "success" is hard to evaluate. Engaging, informing, persuading and influencing can take time: sometimes months, but often many years. Reducing Pashtun support for the Taliban is something that could easily take years or even decades, for instance, and it's certainly unlikely to be accomplished within a single budget cycle. Change is often hard to measure (the Taliban may not feel inclined to take part in focus groups), and meaningful benchmarks difficult to identify. What's more, it's very difficult to disentangle causation and correlation when it comes to SC and IO. If Pashtun support for the Taliban drops and the Taliban begins to struggle to recruit and retain fighters, is this because of SC and IO efforts, or because economic development programs have created alternative livelihoods for young men, or because Taliban leaders have overreached, or because of something else? Often, there's no way to know.

This doesn't mean we shouldn't strive to evaluate the impact of our programs – we should and we must. But it does mean that we need to avoid an obsession with metrics. Accountability for dollars and programs is important, but we should resist the urge to develop simplistic quantitative measures of success or failure. This stuff is hard.

8. We need to decentralize. Strategic communication needs to be part of a broader and well-understood strategy, but messages can't be too top down or tightly controlled. We need to trust each other more, which means, for the White House and for senior leaders in general, letting go of a fixation on "controlling the message." Messages that are overly controlled are often not very persuasive or effective, since by definition they can't be tailored to specific audiences and contexts. We need to give our people the flexibility to adapt messages and programs based on local knowledge, feedback and circumstances. This creates some risk; the more we decentralize, the more likely it is that someone, somewhere, will make a bad decision. But that can't be helped: the risks of over-controlling almost always outweigh the risks of decentralizing.

Decentralization also means we need less naval-gazing obsession with who does what. While it's true that the "right messenger" can be as important as the right message, determining which agency or actor should take on which task should be based on a clear-eyed understanding

on the local context, not on formalistic and mechanical assertions that "the military should never do X" or "It's the State Department's job to do Y." We have real and urgent government-wide needs to develop effective strategic communication strategies, squabbling over the roles of different executive branch agencies is generally a waste of time.

In an ideal world, State should be far better funded, and should be able to recruit and retain a far larger cadre of dedicated, well-trained officials. That would be nice, and I hope we will get there; those in Congress who would like to see the State Department do more than it currently does have a simple expedient, which is to give State some more money. But in the meantime, we might as well let a thousand flowers bloom within the executive branch. If the State Department lacks the funds or capacity to undertake programs or activities that are manifestly in the national interest, then other agencies should step in. If "whole of government" means anything at all, it must mean getting beyond petty squabbles about roles. The mission is too important.

8. There are some things the US Government can't, won't or shouldn't do, but that may be appropriate for NGOs, universities or the private sector. The USG is too bureaucratic to act with agility or sensitivity in certain situations, and sometimes internal politics dictate inaction even when circumstances seem to cry out for action. There are times when USG actors, regardless of agency, simply won't be credible, and there are also times when SC or IO call out for skills that are rearely resident within the USG. That means we need to develop more sustained and robust mechanisms for linking up with the private sector.

Areas for Investment

As the points above suggest, operating in the information environment is difficult, and no panacea. And though investing in effective strategic communication will surely always be cheap relative to new aircraft carriers and fighter jets, it's not something that can be done well on the cheap. So far, however, the USG has not invested significant resources in SC or IO: funding has been haphazard, and training equally so.

What would it mean for this country to get serious about SC and IO?

First and foremost, we need to ensure adequate funding for linguistic, regional and cultural training, both for our military and foreign service personnel, of course, but also in our civilian schools and universities more broadly. During the Cold War, the US Congress appropriated substantial funds for universities to start language and area training programs. Most of that money is long gone, and we now risk having a population that can't find Iraq, Afghanistan or Libya on a map, much less hope to communicate with anyone from one of these countries—or from China or India or any number of key partner states or rising powers, for that matter. Operating effectively in the information environment requires more than a six month language course here and there: if we're serious about engaging credibly with foreign audiences and stakeholders, we need to invest in creating a critical mass of citizens with deep knowledge of other languages and cultures.

We should also invest in programs designed to harness the language and cultural skills that so many of our citizens already possess. Historically, America's strength has been the incredible diversity of our people, who come to this country from all corners of the globe. We've done a shockingly haphazard job of motivating those with key linguistic and cultural skills to

enter public service. We should find creative ways to incentivize citizens who possess key skills to work for the USG, and this too will require an investment of resources.

We also need more old-fashioned public diplomacy: exchange programs, cultural programs, educational programs. People-to-people ties do matter, and we need to have more confidence both in our own people and in foreign publics. The budget cuts in public diplomacy program in the last decades have been nothing short of shameful, as well as deeply short-sighted. Foreign assistance, whether it takes the form of food aid or cultural programs, isn't an act of charity. It's a vital means of advancing our national interests, of building good will and developing the strong networks of friends and information sources that will stand us in good stead when hard times come-- as they will. Are there risks in greater openness, more exchanges and people-to-people ties? Certainly: every now and then, we'll trust someone we shouldn't trust, and pay a price. But as ever, it's an issue of accepting some tactical risk for strategic gain. In the long run, we isolate ourselves at our own peril.

Self-styled realists will argue that we shouldn't obsess too much about inducing foreign publics to "like' us. As long as they don't attack us or aid our enemies, say the realists, it doesn't much matter if other people like us or not. There is plenty of wisdom in this—if the protesters in Egypt's Tahrir Square reject terrorism, that's much more important than "liking" the United States.

But it's true only up to a point. An obsession with being loved and appreciated is not a good basis for strategic communication: sometimes people won't like our policies, and we will have principled reasons for being unwilling to change them, and that's that, and as it should be. But there is a difference between trying to generate a shallow "liking" versus trying to generate confidence and respect, even in the face of inevitable differences. There does appear to be a strong correlation between positive feelings about the United States and fewer attacks against US interests. Being liked is overvalued, and often impossible in a world where conflicting interest are inevitable. But efforts to build trust and understanding do pay off.

Increasing old-fashioned public diplomacy takes money and, at times, political courage. It's not easy to argue for increasing visas for people from Arab and Muslim countries when letting in a single bad actor could lead to an intense backlash. It's not easy to argue for more funds for cultural activities or economic aid overseas when people are hurting here at home. But in each case, we need to understand our activities as investments that will pay off over a longer time frame. If we under-invest now, it will be too late later.

Although I cautioned earlier against an obsession with quantitative metrics, we also need to invest in develop better indicators of impact. Right now, SC and IO programs sometimes seem like so much spaghetti lobbed at the walls: some sticks, some doesn't, and we don't have a very good sense of which factors make the difference. While certaintly may be impossible, getting better at understanding the circumstances in which different approaches may succeed or fail is worthwhile, and will take resources.

Finally, we need to invest in identifying and creating better vehicles for public-private collaboration. Right now, private actors from NGOs to tech or media companies have no systematic way to interact with the USG to identify ways to engage. This is partly a matter of structure and bureaucracy, but partly a matter of resources: right now, it's no one's job to develop and nurture public-private relationships, no one's job to provide information or resources to NGOs or universities interested in building programs that would further US SC or

public diplomacy goals. This could be changed; it's not difficult to imagine developing programs or organizations designed to harness and faciliate private sector action that's in the broader US interest. Here too, the dollar amounts needed to change this are small relative to high tech systems, but large relative to the budgets of most public diplomacy and IO teams. But this is another small investment that could yield big dividends.

Conclusion

I'll wrap these remarks up here. I've touched on a lot of issues, and at the same time, I recognize that I have only begun to scratch the surface. When it comes to producing effects in the information environment, "getting it right" isn't easy. I believe, though, that the potential payoffs are significant. Perhaps more to the point, the costs of getting it wrong are high. I doubt it will have escaped anyone's attention that many of the key capabilities need to get SC and IP right are also key capabilities if we want to get COIN, stability operations, or ordinary diplomacy right: sound strategy, consistency, credibility, decentralization and agility, language and culture skills. If we invest in getting it right in the information environment, there will be spillover effects across a range of other efforts. Conversely, if we can't get it right in the information environment, odds are we'll perform badly across the board. With the security environment growing ever more complex, that's something we can't afford.